The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/02/2016

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome prior to 55.0.2883.75

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- Private property access in V8 (CVE-2016-9651)
- Universal XSS in Blink (CVE-2016-5208, CVE-2016-5207, CVE-2016-5205, CVE-2016-5204)
- Same-origin bypass in PDFium (CVE-2016-5206)
- Out of bounds write in Blink (CVE-2016-5209)

- Use after free in PDFium (CVE-2016-5203, CVE-2016-5211, CVE-2016-5216)
- Out of bounds write in PDFium (CVE-2016-5210)
- Local file disclosure in DevTools (CVE-2016-5212)
- Use after free in V8 (CVE-2016-5213, CVE-2016-5219)
- File download protection bypass (CVE-2016-5214)
- Use after free in Webaudio (CVE-2016-5215)
- Use of unvalidated data in PDFium (CVE-2016-5217)
- Address spoofing in Omnibox (CVE-2016-5218, CVE-2016-5222)
- Integer overflow in ANGLE (CVE-2016-5221)
- Local file access in PDFium (CVE-2016-5220)
- CSP Referrer disclosure (CVE-2016-9650)
- Integer overflow in PDFium (CVE-2016-5223)
- Limited XSS in Blink (CVE-2016-5226)
- CSP bypass in Blink (CVE-2016-5225)
- Same-origin bypass in SVG (CVE-2016-5224)
- Various fixes from internal audits, fuzzing and other initiatives (CVE-2016-9652)

Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Google:
https://googlechromereleases.blogspot.com/2016/12/stable-channel-update-for-desktop.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5203
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5204
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5205
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5206
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5207
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5208
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5209
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5210
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5211

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5212
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5213
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5214
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5215
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5216
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5217
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5218
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5219
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5220
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5221
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5222
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5223
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5224
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5225
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5226
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9650
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9651
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9652